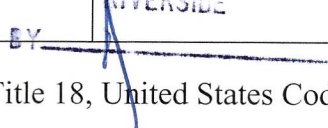
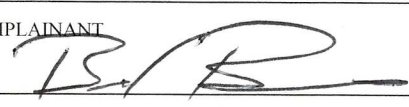



**ORIGINAL**

AO 91 (Rev. 11/82)

**CRIMINAL COMPLAINT**

UNITED STATES DISTRICT COURT		CENTRAL DISTRICT OF CALIFORNIA	
UNITED STATES OF AMERICA v. ANTHONY GARCIA, Defendant.		DOCKET NO. <b>ED-17-0059M</b> 2017 FEB 27 AM 11:44 MAGISTRATE'S CASE NO. CENTRAL DISTRICT OF CALIF. RIVERSIDE BY 	
COMPLAINT FOR VIOLATION OF TITLE 18, UNITED STATES CODE, SECTIONS 1708			
NAME OF MAGISTRATE JUDGE HONORABLE SHERI PYM		UNITED STATES MAGISTRATE JUDGE	LOCATION Riverside, California
DATE OF OFFENSE February 7, 2017	PLACE OF OFFENSE Riverside County	ADDRESS OF ACCUSED (IF KNOWN)	
COMPLAINANT'S STATEMENT OF FACTS CONSTITUTING THE OFFENSE OR VIOLATION: <p style="text-align: center;">[18 U.S.C. § 1708]</p> <p>On or about February 7, 2017, in Riverside County, within the Central District of California, defendant ANTHONY GARCIA unlawfully had in his possession mail which had been stolen from the mail or a mail receptacle, addressed to and from persons other than defendant, knowing the same to have been stolen.</p>			
BASIS OF COMPLAINANT'S CHARGE AGAINST THE ACCUSED: <p style="text-align: center;">(See attached affidavit which is incorporated as part of this Complaint)</p>			
MATERIAL WITNESSES IN RELATION TO THIS CHARGE: N/A			
Being duly sworn, I declare that the foregoing is true and correct to the best of my knowledge.		SIGNATURE OF COMPLAINANT <b>Brad Barnes</b> 	
		OFFICIAL TITLE U.S. Postal Inspector – U.S. Postal Inspection Service	
Sworn to before me and subscribed in my presence,			
SIGNATURE OF MAGISTRATE JUDGE <sup>(1)</sup> 		DATE February 27, 2017	

<sup>(1)</sup> See Federal Rules of Criminal Procedure 3 and 54

AFFIDAVIT

I, Brad Barnes, being duly sworn, declare and state as follows:

I. PURPOSE OF THIS AFFIDAVIT

1. This affidavit is made in support of a criminal complaint against and arrest warrant for Anthony Garcia ("GARCIA") for a violation of Title 18, United States Code, Section 1708 (Possession of Stolen Mail).

2. This affidavit is also made in support of an application for a warrant to search the digital device described in Attachment A ("GARCIA'S TELEPHONE"), which is incorporated by reference herein.

3. The requested search warrant seeks authorization to seize any data on GARCIA'S TELEPHONE that constitutes evidence, fruits, or instrumentalities of violations of 18 U.S.C. § 1704 (Possession of Counterfeit United States Postal Service Arrow Key), 18 U.S.C. § 1708 (Mail Theft and Possession of Stolen Mail), 18 U.S.C. § 371 (Conspiracy), 18 U.S.C. § 1344 (Bank Fraud), 18 U.S.C. § 1028 (Fraud and Related Activity in Connection with Identification Documents, Authentication Features, and Information), 18 U.S.C. § 1029 (Access Device Fraud), and 18 U.S.C. § 1028A (Aggravated Identity Theft), as more fully described in Attachment B, which is incorporated herein.

4. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel,

including members of the Beaumont Police Department ("BPD"). This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint, arrest warrant, and search warrant, and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

**II. BACKGROUND FOR POSTAL INSPECTOR BRAD BARNES**

5. I am a United States Postal Inspector ("Postal Inspector") employed by the Los Angeles Division of the United States Postal Inspection Service ("USPIS"), San Bernardino Domicile, External Crimes Team. I have been so employed since July of 2013. My responsibilities include the investigation of crimes against the United States Postal Service ("USPS") and crimes related to the misuse and attack of the mail system and assaults and threats against USPS employees, including: theft of United States mail ("U.S. Mail"); possession of stolen United States mail; crimes related to the use, theft, and counterfeiting of postal keys (referred to as "arrow keys") and locks; access device fraud; and identity theft. Additionally, I have received both formal and informal training from the USPIS regarding mail and identity theft.

6. Through my training and experience, I have learned that USPS provides large blue collection boxes as a convenient receptacle for USPS customers to mail their correspondence to others. In my training and experience, I have also learned that

mail thieves target these blue collection boxes to steal mail. Non-postal employees and mail thieves commonly call the method of stealing from the blue collection boxes "fishing". Fishing is done by the mail thief using a long string or strap with a heavy device attached on the end. The heavy device is covered with a sticky substance, usually obtained from the glue of a rat trap. The sticky end of the device is lowered into the blue collection box and mail gets stuck to the end. The mail thief then pulls the device out and obtains the mail. As a result of stealing mail, mail thieves can gain access to items such as checks, money orders, cash, and gift cards, as well as individuals' personal information, and use such information to commit bank fraud, check fraud, and access device fraud with credit cards and debit cards.

### III. SUMMARY OF PROBABLE CAUSE

7. On February 7, 2017, at approximately 11:37 p.m., while on patrol in Beaumont, California, Beaumont Police Department ("BPD") Detective Marquez stopped GARCIA for several traffic violations. GARCIA consented to a search of his car, and Officer Marquez found over 120 personal checks to and from people other than GARCIA, two credit cards in names other than GARCIA's, a tax return in a name other than GARCIA's, three postal keys, and two flat head screw drivers.

8. In a subsequent interview, GARCIA admitted to stealing mail with a co-conspirator, stealing and attempting to cash stolen checks, and using his telephone to contact people in order to sell stolen checks.

IV. STATEMENT OF PROBABLE CAUSE

9. Based on my review of investigative reports and discussions with members of the BPD, I am aware of the following:

A. Initial Beaumont Police Department Traffic Stop

10. On February 7, 2017, at approximately 11:37 p.m., BPD Detective Marquez, was travelling west on the Interstate 10 Freeway when he saw a black Acura TL with dealer plates ("GARCIA'S CAR") pass him traveling at approximately 80 miles per hour in a 65 MPH speed limit zone. Detective Marquez recognized the activity as a violation of California Vehicle Code ("CVC") Section 22350. Detective Marquez also noticed that GARCIA'S CAR wove in and out of the number 1 and number 2 lanes without signaling, as it passed slower moving cars at a high rate of speed, a violation of CVC Section 22107 (Unsafe turn), and CVC Section 22108 (Failure to Signal 100 feet before Turning). In addition, Detective Marquez saw that the front windows had dark window tint, which completely obscured his view into the car, a violation of CVC Section 26708.5 (Dark window tint). Based on these violations, Detective Marquez initiated a traffic stop on GARCIA'S CAR.

11. GARCIA'S CAR did not immediately pull over and instead began to slow down as the driver, later identified as Anthony Garcia ("GARCIA"), activated the car's emergency lights. GARCIA'S CAR was slightly weaving side to side and continued traveling westbound. The Acura then suddenly pulled off the

freeway and exited at Singleton Road, and subsequently stopped on the shoulder.

12. Detective Marquez approached GARCIA'S CAR from the driver's side. Due to the dark window tint Detective Marquez asked GARCIA to roll down the windows. GARCIA then opened the driver's side door and told Detective Marquez he was sorry for speeding.

13. Detective Marquez asked to see his driver's license. GARCIA gave Detective Marquez a CA identification card and registration, which returned to an Acura, California license plate number "5WTG555," registered to GARCIA. The registration had expired in 2014, in violation of CVC 4000 (a)(1) (Expired registration).

14. Detective Marquez noticed a strong odor of marijuana coming from the car and asked GARCIA if he had anything illegal on his person or the car, including drugs and weapons. GARCIA hesitated to answer.

**a. Search of GARCIA's Car**

15. Detective Marquez asked GARCIA to exit the car in order to safely conduct his investigation.

16. GARCIA told Detective Marquez that he had marijuana in the center console. Detective Marquez asked GARCIA if he had anything else illegal in the car. GARCIA said that he may have a taser weapon somewhere the car.

17. Detective Marquez asked GARCIA if he could search the interior of the car for anything illegal. GARCIA gave verbal

consent. During a search of the car, Detective Marquez found the following:

- a. marijuana residue located on the driver's side seat;
- b. a black container that had a small amount of marijuana in the center console;
- c. a glass pipe, used for smoking, that contained burned marijuana on the front passenger's seat;
- d. GARCIA'S TELEPHONE in the center console;
- e. an orange envelope in the sunroof area, with a return address to M.O. on Raven Ln in Lancaster, California on the top left corner and addressed to the Department of Treasury in Kansas City, Missouri in the sunroof area. Located inside the envelope were the following:
  - i. Approximately 100 personal checks from different people from various cities including Bakersfield and Las Vegas. Some of the checks had personal account holder information such as bank account numbers, addresses and phone numbers. The checks were written to utility companies in the corresponding areas;
  - ii. A shipping envelope bearing GARCIA's name and address. Located in the shipping envelope were two credit cards issued to U.C.
- f. A white envelope concealed under the center console. The envelope displayed the name R.C. with an address in Bakersfield, California. The envelope was addressed to



another subject with an address also in the Bakersfield area. The envelope contained the following:

- i. Approximately 17 personal checks from different people in the Bakersfield area. Some of these checks also appeared to have personal account holder information such as bank account numbers, addresses and phone numbers. The checks were written to utility companies in the corresponding areas;

- ii. A tax return from a resident in the city of Bakersfield. The tax return form contained personal identifying information such as a social security number;

- iii. Mail addressed to a subject from the Los Angeles area.

- g. A brown McDonalds paper bag located in the back seat. Inside the McDonalds paper bag were the following:

- i. Approximately nine personal checks from various people with addresses in the Cathedral City area. Some of the checks included personal account holder information such as bank account numbers, addresses and phone numbers;

- ii. Mail from a business Palm Café, located in the city of Rancho Mirage;

- iii. A Los Angeles court letter addressed to GARCIA.

- h. A black jacket on the back seat, which contained three post office keys. One of the keys had the imprint "U.S.P.S. DO NOT DUPLICATE."

- i. Two flat head screw drivers in the car's trunk.



18. While on scene, Detective Marquez reviewed a personal check that was found in the orange envelope. The check displayed the name C.A. with an address in the city of Bakersfield, California. The check displayed a phone number for C.A. Detective Marquez contacted C.A. via telephone. C.A. told Detective Marquez the following:

a. On January 28, 2017, C.A. put the checks found in GARCIA's possession into a blue collection box outside of the Bakersfield post office located at 3200 Larson Lane in the city of Bakersfield, California.

b. C.A. wrote the checks for utility/mortgage payments for over \$900.

c. C.A. believes an unknown suspect stole his checks from the blue collection box.

d. C.A. does not know GARCIA and never gave GARCIA permission to possess his checks.

19. In total, during the search, Detective Marquez and Marsh identified approximately 126 personal checks with issued payments totaling approximately \$32,000.

20. GARCIA was placed under arrest and transported to the BPD. GARCIA'S CAR was towed by Empire Towing.

**b. GARCIA's Statements**

21. At the station, Detective Marquez advised GARCIA of his Miranda Rights. GARCIA agreed to speak to Detective Marquez and provided the following information:

a. Approximately one month prior, GARCIA met a male who goes by the name "The Plug" at a business in the South

Central Los Angeles area. GARCIA does not know The Plug's real name. GARCIA began using methamphetamine with The Plug every time GARCIA was with him.

b. The Plug would contact GARCIA by telephone and ask to meet at local stores in the South Central Los Angeles area.

c. The Plug offered to fill GARCIA's gas tank and give him money if GARCIA would give him rides to places. GARCIA agreed and drove The Plug to different cities in Los Angeles to steal from mailboxes.

d. GARCIA has been driving The Plug around to steal from mailboxes for the past month.

e. GARCIA drove The Plug to Bakersfield and Las Vegas, where they also stole mail from mailboxes.

f. The Plug would use GARCIA's cellular phone to contact various people in order to sell the stolen checks.

g. The Plug would fill up GARCIA's car's gas tank and also give GARCIA approximately \$100 in cash from the money made by selling the stolen checks.

h. The Plug steals mail from mailboxes in the vicinity of Cathedral City.

i. The Plug gave GARCIA one of the stolen checks so he could cash it. The Plug was able to alter the check and write GARCIA's name as the payee on the stolen check for the amount of \$500.

j. GARCIA attempted to cash the stolen check at a bank in the Cathedral City in an attempt to obtain \$500 cash from the check's account holder.

k. GARCIA knew the check was stolen while attempting to cash it.

l. The credit cards issued to "U.C." belong to GARCIA's friend.

m. The Plug tried to use the postal keys to break into mailboxes, but they did not work.

n. The Plug gave the keys and stolen checks to GARCIA to hold because The Plug did not want to get caught with them in his possession.

o. The Plug hid the envelopes in GARCIA's car.

**c. Follow-up Investigation**

22. On February 9, 2017, I met with Detectives Marquez. Detective Marquez provided me a copy of his report for further investigation.

23. On February 10, 2017, I interviewed Detective Marquez regarding the case. Detective Marquez told me the following:

a. GARCIA's cell phone is a black Samsung Cellular phone displaying model number SM-N910T and serial number RF8FC0LEZ6W.

b. During the initial contact with GARCIA, prior to searching the car, Detective Marquez asked if GARCIA had anything in the car he was not supposed to have. GARCIA replied, "You could go in and search." Detective Marquez asked GARCIA if there was anything in the car besides the marijuana.

GARCIA nodded his head from side to side and mumbled, "You can check."

24. TRAINING AND EXPERIENCE REGARDING THE MAIL THEFT AND BANK FRAUD

25. Based on my knowledge, training, and experience, as well as information related to me by other law enforcement officers and Postal Inspectors, I know that:

a. Mail thieves often use stolen or counterfeit arrow keys and/or pry tools, such as crow bars or screw drivers, to gain access to neighborhood mailboxes in order to steal mail from numerous mailboxes at one time. Mail thieves also "fish" out of USPS collection boxes in order to steal US Mail. As a result of stealing mail, mail thieves can gain access to items such as checks, money orders, cash, and gift cards, as well as individuals' personal information and identification documents, and use such information to commit bank fraud, check fraud, and access device fraud with credit cards and debit cards.

b. It is common practice for mail and identity thieves to keep "profiles" of victims, including on their digital devices. Such "profiles" contain the personal identifying information of victims, such as names, Social Security numbers, dates of birth, and driver's license or state identification numbers, alien registration numbers, passport numbers, and employer or taxpayer identification numbers.

c. Individuals who participate in mail and identity theft use digital devices to maintain telephone numbers of co-conspirators in order conduct their business, to communicate

with co-conspirators, and to coordinate their activities. Individuals often communicate with their co-conspirators by phone, e-mail, text message and social media.

V. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

26. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that it is not always possible to search digital devices for digital data in a single day or even over several weeks for a number of reasons, including the following:

a. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. There are so many types of digital devices and software programs in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. As a result, a controlled environment, such as a law enforcement laboratory

or similar facility, is essential to conducting a complete and accurate analysis of data stored on digital devices.

c. The volume of data stored on many digital devices will typically be so large that it will be highly impractical to search for data during the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 500 or more gigabytes are now commonplace. Consequently, just one device might contain the equivalent of 250 million pages of data, which, if printed out, would completely fill three 35' x 35' x 10' rooms to the ceiling. Further, a 500 gigabyte drive could contain as many as approximately 450 full run movies or 450,000 songs.

d. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files saved to a hard drive can be stored for years with little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, i.e., space on a hard drive that is not allocated to an

active file or that is unused after a file has been allocated to a set block of storage space, for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a swap or recovery file. Similarly, files that have been viewed on the Internet are often automatically downloaded into a temporary directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently downloaded or viewed content. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Recovery of residue of electronic files from a hard drive requires specialized tools and a controlled laboratory environment. Recovery also can require substantial time

e. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processing, picture, and movie files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications and materials contained on the digital devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregated from the hard drive image



as a whole. Digital data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

f. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone

else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data on a digital device is not segregated from the digital device. Analysis of the digital device as a whole to demonstrate the absence of particular data requires specialized tools and a controlled laboratory environment, and can require substantial time.

g. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband or instrumentalities of a crime.

27. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

28. CONCLUSION

29. Based on the foregoing facts, there is probable cause to believe that Anthony GARCIA and other unknown persons have committed a violation Title 18, United States Code, Section 1708 (Theft and Possession of Stolen Mail) and for violation of Title 18, United States Code, Section 371, (Conspiracy to Steal or Receive Stolen Mail).

30. For the reasons described above, I respectfully submit there is probable cause to believe that evidence, fruits, and instrumentalities of the Subject Offenses will be found on the GARCIA'S TELEPHONE.



Brad Barnes, Postal Inspector  
United States Postal Inspection  
Service

Subscribed to and sworn before me  
this 27<sup>th</sup> day of February, 2017



UNITED STATES MAGISTRATE JUDGE